DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Name Redacted]	)	ISCR Case No. 15-08717
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Rhett Petcher, Esq., Department Counsel
For Applicant: *Pro se*

02/06/2017

_____

Decision

_____

HOGAN, Erin C., Administrative Judge:

On August 15, 2016, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline K, Handling Protected Information. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the Department of Defense after September 1, 2006.

On August 26, 2016, Applicant answered the SOR and requested a hearing before an administrative judge. Department Counsel was ready to proceed on October 14, 2016. The case was assigned to me on October 28, 2016. On November 9, 2016, a Notice of Hearing was issued, scheduling the hearing for December 5, 2016. The hearing was held as scheduled. During the hearing, the Government offered four exhibits which were admitted as Government Exhibits (Gov) 1 – 4. Applicant testified and called one witness, but offered no exhibits. The transcript (Tr.) was received on December 13, 2016. The record was held open until December 19, 2016, to allow Applicant to submit documents. Applicant submitted documents which were marked as

Applicant Exhibits (AE) A – H. Department Counsel had no objection to AE A – G, but objected to AE H as an exhibit, but does not object to AE H being considered as Applicant's written closing argument. I sustain Department Counsel's objection and admitted AE H for the limited purpose of Applicant's written closing argument. Based upon a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

Findings of Fact

In his response to the SOR, Applicant admits SOR ¶ 1.a(iii) and denies the allegations in SOR ¶¶ 1.a(i), 1.a(ii), and 1.b. In the interests of Applicant's privacy, generic terms are used in the body of the decision. More specific details can be found in the record evidence.

Applicant is a 61-year-old employee of a DoD contractor seeking to maintain a security clearance. He has worked for his current employer since March 1987. He has a Master's Degree in Electrical and Computer Engineering. He has held a security clearance since 1985. He is married and has two adult children. (Tr. at 26-27; Gov 1)

In September 2015, Applicant was found culpable of three security violations. The most serious violation occurred between November 2014 and May 2015. In July 2015, a government office notified Applicant's employer classified information was discovered during a review of program material, which the employer was requesting approval for public release. The information involved an [advanced system] which was classified as confidential. The image sent to the government office for public release was a screen shot taken during a live demonstration for a foreign military. A government employee recognized that the company did not have proper licensing to display classified information to the foreign military and contacted Applicant's employer to initiate an investigation into the disclosure issue. (Gov 4)

In August 2014, Applicant served as a Chief Engineer and the liaison to a committee consisting of representatives of each U.S. military service (Committee). He initiated discussions with the Committee to gain approval to update the [advanced system's] marketing material for a proposed briefing that would take place with foreign customers. Applicant wrote a technology control plan (TCP) which outlined what would be viewed by each foreign customer. The TCP prohibited the display of [certain confidential information]. (Gov 4 at 4)

Applicant wrote two documents related to the marketing demonstration. The first was a power point presentation which provided an overview of the planned customer visits to the test site. The second was the TCP which was more detailed and outlined where the customers would be going and what they would and would not have access to. Applicant specifically stated in each document that the [confidential information] was not to be shown." The TCP was provided to Mr. A, the program manager, who composed an invitation for a demonstration to take place on November 19, 2014, for

foreign government officials. Mr. A. requested all employees involved to review the TCP prior to the demonstration to understand the "run rules." (Gov 4 at 4)

Applicant attended four subsequent demonstrations with foreign nationals where the [confidential information] was displayed in violation of the TCP. The demonstrations occurred on November 9, 2014, December 15, 2014; April 15, 2015, and May 14, 2015. No one present at any of the demonstrations identified the issue of the [confidential information] being displayed. (Gov 4 at 4)

Applicant and Mr. A., the program manager, were both interviewed by security after the security violation. Neither could recall that the [confidential information] was displayed during the demonstrations. Security also interviewed Mr. B., an engineer who was running the demonstration during each customer visit and who created the script of each presentation. Mr. B. said he kept in the [confidential information] because he believed it was unclassified based on his understanding of the [advanced system] classification guide and his 20 years experience as an [advanced system] engineer. He takes full responsibility for concluding the [confidential information] was unclassified and said that no one in the program forced his decision. He only glanced at the TCP and did not read the section discussing the [confidential information]. (Gov 4 at 4)

During the investigation, it was discovered that two classified Committee memos were received by Applicant in September 2014. One was a draft and the other was the signed final copy. The draft copy was not accounted for by Document Control. Applicant was re-interviewed about the draft document. Applicant believes that he placed the draft copy in his classified working papers which were dropped off at Document Control to be destroyed. The Security Office concluded that document was lost because there was no proof that the document was destroyed by Applicant or the Accountable Information Management System. (Gov 4 at 5, 9-11)

The investigation determined that three senior level employees failed to mitigate the release of classified information to foreign nationals, which violated the NISPOM and other security regulations. Applicant was disciplined for two separate security violations and received one month's suspension and no supplemental compensation for 2015. Mr. A. was suspended for two weeks and his 2015 supplemental compensation was reduced by 50%. Mr. B. received a two week suspension and his 2015 supplemental compensation was reduced by two weeks. All three senior level employees were re-briefed on their responsibilities to protect classified information. Multiple team members were present during these demonstrations. They failed to identify the [confidential information] as well. They received counseling and training to avoid similar incidents in the future. (Gov 4 at 6)

During the investigation, two other security incidents were discovered involving Applicant. One of the employees who was interviewed about the foreign visitors incident, volunteered that Applicant hosted an unclassified meeting on July 30, 2015, to meet the new Army representative to the Committee. At some point in the meeting, the Army representative asked a question. The only way to answer the question was to

provide a classified answer. Applicant was asked if it was okay to provide the answer. Applicant gave permission to provide the classified answer even though the meeting was scheduled as an unclassified meeting. Applicant told security investigators that he gave permission to provide the classified answer because he believed the Army representative was cleared based on the fact that he had attended previous classified meetings with the Army representative. Applicant was aware of the process to follow when conducting a classified meeting. He was aware of the requirement to properly verify clearances through security before a classified meeting. However, he knew the Army representative and did not think his security clearance was an issue. Later, the security office contacted the Army representative's security office and his security clearance was verified. It was concluded the classified information was not vulnerable to disclosure because the Army representative had a current Top Secret security clearance and a need to know the information. (Gov 4 at 13-14)

The second incident occurred before Applicant started his four-week suspension on September 28, 2015. On September 24, 2015, an inventory was conducted on Applicant's classified container in order to account for all of his classified documents before he left. One secret document was missing. Applicant said he turned in this document to Document Control the day before (September 23, 2015) for destruction. Ms. M., a document control employee, recalls receiving documents from Applicant, but does not recall receiving the missing secret document as one of the items. Applicant said he informed Ms. M. about the document and asked if there were special procedures for its disposition. He was told there was not. He was not asked to complete a hand receipt for the document requesting that it be destroyed, which according to security was the standard process for turning accountable material into document control. (Gov 4 at 17-18)

Ms. M. provided all classified material to her manager for destruction. He did not check the documents or CDs for accountability numbers because he assumed Ms. M. had already conducted a review. It could not be confirmed that the missing secret document was destroyed. The security office concludes a document is lost when this occurs. Applicant was found partially culpable because it was his responsibility to request a receipt when transferring accountable classified material. As a result of this incident, a new process was instituted in Document Control that required two employees to verify that every classified item being destroyed is thoroughly reviewed to ensure accountable information is not mixed with unaccountable working papers. (Gov 4 at 18-19)

The investigation concluded Ms. M. did not follow standard Document Control processes. She accepted classified material for destruction from Applicant without preparing a classified material hand receipt to document the transaction. Ms. M. received a one- week suspension without pay. This was her second security violation in a 12-month period regarding a missing classified document. In November 2014, she shared culpability with another employee, who believed he turned in a classified document to Document Control for destruction, but was not provided a hand receipt to document the transaction. (Gov 4 at 23)

The security office recommended that Applicant be terminated from employment because this was his fourth NISPOM violation and second lost classified document within a two month period. They contend Applicant has shown a pattern of negligent behavior and carelessness for handling classified information. (Gov 4 at 23) Prior to these incidents, Applicant had no previous security violations during his over 30 years of handling classified information. (Gov 4)

Applicant's Response to SOR Allegations:

SOR ¶ 1.a(i): Applicant denies the allegation in SOR ¶ 1.a(i). He claims that the [confidential information] was redacted from the demonstration during dry runs prior to the foreign customer demonstrations. He did not notice that the [confidential information] was displayed during the foreign customer demonstrations. Applicant said his role in the foreign customer demonstration was a support role. At the direction of the Committee, he provided a written TCP to the Program Manager for distribution and implementation by his team in preparation for the visits. Applicant had no part in creating or executing the actual test event. Applicant states that between 10 to 15 people were present during each demonstration consisting of the foreign customers, fellow employees and technical representative from the U.S. government. No one else raised the issue of the [confidential information] being present during the foreign customer demonstrations. (Answer to SOR; Tr. 16-19, 27-34, 46, 49-50)

There was a debate as to whether the [confidential information] in question was actually classified. It was not until the company was attempting to get a public release of the demonstration where a photograph taken of the display with a foreign general sitting in front of the display that someone raised the issue about the [confidential information] being classified as secret. It was later determined it was classified as confidential. (Tr. 49-50)

SOR ¶ 1.a(iii): Applicant admits that he demonstrated poor judgment when he vouched for the new US Army representative of the Committee during an unclassified meeting in July 2015 and allowed classified information to be provided during the meeting without going through proper channels to verify the US Army representative's security clearance. Applicant had attended previous meetings with him and knew that he was cleared to the proper classification level. It was later confirmed that the US Army representative was cleared. Applicant admits he should have confirmed the new US Army representative had the clearance before he gave the information. (Tr. 14-16, 38-40)

SOR ¶ 1.a(ii): The SOR alleges Applicant lost a draft classified Committee Decision Memo that had been superseded by the final classified Decision Memo one week later. Applicant denies the allegation. Applicant believes he returned this draft document to the Document Control center for destruction with other working papers. The document was assigned a control number and was assigned to Applicant as a custodian. The working papers were not assigned control numbers. Applicant believes it

is most likely the accountable document was destroyed with the working papers. Applicant states that Document Control did not have a process for documenting the return of a controlled document for destruction. He was not given a receipt and cannot prove that the document was returned to Document Control for destruction. (Response to SOR, Tr. 20-22, 35-37, 42)

SOR ¶ 1.b: The SOR alleges in September 2015, it was discovered that Applicant lost another classified document during an inventory of Applicant's security container the day before he began his 30-day suspension. Applicant denies this allegation. The day before the inventory of his security container, Applicant had been notified that a particular program was terminated and if he wanted to retain a classified document that was in his safe, he would need to request permission to keep it or have it destroyed. Applicant indicated that he would have the document destroyed. He took the document to Document Control. He vividly remembers that he told Document Control personnel (specifically Ms. M.) that this document was from an expired program in case it needed to be handled with different record keeping. He was told that it did not. He denies Ms. M.'s contention that he did not tell her that the document was a special document. Applicant states that the system in place at the time provided no record or receipts for the document. You would be notified several weeks after you dropped off controlled documents that the documents were destroyed. In his security training, he was never told that it was his responsibility to get a receipt when he turns in controlled documents to Document Control for destruction. He believes both documents were not lost, but destroyed without being accounted for as being destroyed. He tracked the document up to the time he provided the documents to Document Control. He relied on the subject matter expertise of Document Control personnel to provide guidance. (Response to SOR, Tr. 23-25, 42-46)

Whole-Person Factors

Mr. X. works with Applicant. His views are his own and do not represent the views of Applicant's employer. Mr. X. is a security manager. He is a retired Chief Warrant Officer from the U.S. Coast Guard. During his service in the Coast Guard, he had extensive experience in handling security matters. He is a board certified security management specialist and a certified protection professional. He has extensive experience in protecting and handling classified information and the security clearance process. (Tr. 55-57)

Mr. X. has worked with Applicant for over 10 years. He describes Applicant as a careful, thoughtful, very security conscious employee. He does not believe Applicant is a risk or threat to national security. Previous to Applicant's security incidents, he had no prior history of mishandling classified information. He does not believe Applicant has lost the capacity to exercise good judgment and to protect classified information because of these incidents. He would not have testified on Applicant's behalf if he believed otherwise. He discussed the incidents with Applicant. Applicant understands that he made procedural mistakes that could have put information at risk. (Tr. 59-62)

Mr. X. reviewed the reports on the four security incidents. He does not agree with the outcome of the two incidents where Applicant turned in documents for destruction. Document Control did not communicate to the general population that they must obtain receipts when turning in classified documents for destruction. Applicant would not have expected to receive a receipt because he had no knowledge of the procedure. He claims the likelihood of the loss of both documents is improbable.(Tr. 63-78)

Mr. X. is not condoning Applicant's actions in the other incidents. He discussed with Applicant what needs to be done and why. Applicant received refresher security training after the incidents. He has no concerns with Applicant handling classified information. (Tr. 80-81)

Applicant provided copies of his performance evaluations for 2014 and 2015. (AE A; AE B) In 2014, Applicant was considered to have far exceeded requirements. In 2015, Applicant was considered to have met requirements. The performance evaluation states:

> In closing, [Applicant] had a terrific year by most counts. The one count that tempers my enthusiasm for his accomplishments stems from a series of security/ITAR violations have occurred at [name of facility redacted] that had [Applicant's] direct involvement, and for which [Applicant] was justly punished. I want to go on record of stating that [Applicant's] response to his shortcomings have been nothing short of tremendous. Back in September 2015, I challenged [Applicant] to "serve this punishment professionally, think about how you are going to make overt and visible changes in your attention to detail in upholding security as priority one, and come back to the job you are doing with conviction and renewed purpose." [Applicant] was suspended for one month, and his RBI for Performance Year 2015 was reduced to 0%. While painful for [Applicant] (and for me – because otherwise, [Applicant's] year certainly 'Exceeded" my expectations (and perhaps "Far Exceeded"). However, as is customary for severe security related infractions, [Applicant] is receiving a "M – Met Expectations" rating for 2015. I want to go on record stating that [Applicant] has been nothing but apologetic and regretful for these incidents, and in fact has become one of the most curious, insightful, and inquisitive Engineers on my staff so that he and our entire team understand the evolving EXIM requirements, the training we are taking, and the every day steps in our lives that each of us must take to ensure that we are saluting to those EXIM rules. I am quite proud of [Applicant's] professional behavior despite the sting of this ruling – and I look forward to putting this behind us and seeing [Applicant] return to his strong year-to-year performance like we've come to count on. Thank you [Applicant]. (AE B at 1)

On April 4, 2016, Applicant's Director wrote a letter recommending that Applicant be promoted to the level of Principal Engineering Fellow. The Director worked closely

with Applicant over the last five years and is impressed by Applicant's depth and breadth of his technical knowledge. He states that Applicant has been key to enabling [the company's] success "by collaborating across the company, identifying performance gaps, developing solutions to fill those gaps and finding creative funding opportunities to make these concepts real." He believes Applicant has demonstrated his qualifications to be promoted. (AE C)

On April 15, 2016, a Director, Export Policy, Office of Naval Research, also recommended Applicant for promotion. He states that Applicant's efforts have resulted in ". . . successful government/industry relationship that is mutually respectful and achieves results that provide great benefit to the war fighter." (AE D)

Applicant has taken several courses on security and protecting classified information since these incidents happened to include: DoD Annual Security Refresher Briefing on May 18, 2015, Classified Information System User Briefing on June 28, 2015, SAP/SCI Annual Security Refresher Briefing on May 18, 2015, CERT: SAP/Special Programs Annual Security Refresher Briefing on November 8, 2015. In 2016: LO/CLO Technology and CPI in ITAR Authorizations on April 20, 2016, Coordination with the USG for Disclosure of LO/CLO Technology and COPI on April 20, 2016; DoD Annual Security Refresher Briefing on April 20, 2016; SAP/SCI Annual Security Refresher Briefing on April 20, 2016, CERT: SAP Annual Security Refresher Briefing on November 2, 2016. (AE E; AE F; AE G)

Shortly after the foreign representative demonstration incidents, security training was conducted regarding NISPOM and ITAR regulations through a stand-down provided by security. For the July 30, 2015 violation, Applicant was re-educated on the responsibility and process for verifying security clearance information prior to disclosing classified information. (AE G at 2)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which must be considered when determining an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion as to obtaining a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K, Handling Protected Information

The security concern relating to the guideline for Handling Protected Information is set out in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a security concern.

The guideline notes several disqualifying conditions that could raise security concerns:

> AG ¶ 34(a): deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to

personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;

AG ¶ 34(b): collecting or storing classified or other protected information at home or in any other unauthorized location;

AG ¶ 34(c): loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;

AG ¶ 34(d): inappropriate efforts to obtain or view classified or other protected information outside one's need to know;

AG ¶ 34(e): copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings:

AG ¶ 34(f): viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

AG ¶ 34(g): any failure to comply with the rules for the protection of classified or other sensitive information;

AG ¶ 34(h): negligence or lax security habits that persist despite counseling by management; and

AG ¶ 34(i): failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

With respect to SOR ¶ 1.a(i) relating to the disclosure of the confidential information to uncleared foreign nationals during four separate demonstrations, I find that AG ¶ 34(a), AG ¶ 34(g), and AG ¶ 34(i) apply. AG ¶ 34(a) applies because Applicant was in attendance at all four demonstrations, but failed to notice that the [confidential information] was shown during the demonstration. It is noted that apparently no one present at these demonstrations noticed the presence of the [confidential information] or if they noticed it, they did not stop the demonstration to raise a concern about its classification. Applicant's failure to notice the presence of the [confidential information] was negligent as opposed to deliberate. Regardless, it resulted in the compromise of classified information. AG ¶ 34(g) applies because Applicant failed to comply with the rules for protecting classified or other sensitive information. As the author of the TCP, he was aware that the [confidential information] was not to be displayed during the demonstrations. AG ¶ 34(i) applies for the same reasons. However, the damage to National Security is unknown.

With respect to SOR ¶ 1.a(iii), pertaining to the incident where Applicant vouched for the Army representative's security clearance during an unclassified meeting, AG ¶ 34(g) applies. During the classified meeting, the Army representative asked a question that required a classified answer. Applicant was asked by a subordinate whether they could answer the question. Instead of following the procedures in place to verify that the Army representative had the requisite clearance and the need to know, Applicant allowed the classified answer. Applicant attended previous classified meetings where the Army representative was present and vouched for his security clearance. It is noted that no compromise of classified information occurred during this meeting, because it was later confirmed the Army representative had the requisite security clearance and the need to know the information.

With respect to Applicant being found partially responsible for the loss of classified documents on two occasions (SOR ¶ 1.a(ii) and SOR ¶ 1.b), I do not find Applicant culpable in either incident. Applicant's testimony was credible when he explained that he turned in both documents to Document Control. Both classified documents were likely destroyed, but were not documented by Document Control as a result of a systemic problem. Applicant did not receive a receipt for either document. He was not aware that he was required to obtain a receipt for controlled documents when turning them into Document Control. Although a rule was apparently in place, requiring employees to obtain a receipt when turning in controlled (classified) documents for destruction to Document Control, the new policy was not widely circulated. Mr. X. testified that Applicant would have not been aware of this additional procedure. Document Control encountered similar issues in the recent past regarding the failure to account for controlled documents before they were destroyed. There is nothing in the record evidence which indicates Applicant was properly trained on this procedure. I cannot find Applicant responsible for the loss of the two documents he turned into Document Control because he was not properly trained on the requirement to get a receipt for the controlled documents turned in for destruction.

The Government's substantial evidence and Applicant's own admissions raise security concerns under Guideline K. The burden shifted to Applicant to produce evidence to rebut, explain, extenuate, or mitigate the security concerns. (Directive ¶E3.1.15) An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. (*See* ISCR Case No. 02-31154 at 5 (App. Bd. Sept. 22, 2005))

The guideline also includes examples of conditions that could mitigate security concerns arising from financial difficulties:

> AG ¶ 35(a): so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

> AG ¶ 35(b): the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> AG ¶ 35(c): the security violations were due to improper or inadequate training.

All three mitigating conditions apply. Prior to these security incidents, Applicant held a security clearance for over 30 years with no security violations. Applicant responded favorably to counseling and follow-up security training. Mr. X. testified that he talked extensively with Applicant about the incidents and what he needs to do in the future. Applicant's supervisor, indicated in Applicant's 2015 rating that his response to his security violations "have been nothing short of tremendous." Applicant was "apologetic and regretful" over the incidents and has become the most proactive employee on his staff about educating himself and others about security requirements and making sure the requirements are met. While Applicant was involved in one serious security violation, involving disclosure of classified information to foreign nationals and several minor security incidents, his efforts to learn from his mistakes demonstrate that similar behavior in the future is unlikely to recur. His past mistakes do not cast doubt on his current reliability, trustworthiness, or good judgment. He responded favorably to subsequent security training. If the two incidents involving the failure to obtain a receipt when turning in controlled documents for destruction are considered security violations, then AG ¶ 35(c) applies because Applicant was not given adequate training on the procedure for turning in controlled documents.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered Applicant's 30-year history of favorable duty performance with his current employer. I considered that Applicant responded favorably after the security incidents. He served his thirty-day suspension, but returned to work with a positive attitude. He attended follow-up security training and discussed the incidents extensively with Mr. X., a security professional in his organization. He has learned a valuable lesson about the importance of following the rules to protect classified information. Security concerns under Handling Protected Information are mitigated.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a – 1.b:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

ERIN C. HOGAN
Administrative Judge